U.S. Department of Housing and Urban Development

PRIVACY INCIDENT RESPONSE PLAN

AUGUST 2020

Issue	Date	Pages Affected	Description
Version 1.0	**August 2020**	**All**	**Establishes HUD's Privacy Incident Response Plan for all HUD personnel.**

Table of Contents

Introduction

The HUD Privacy Incident Response Plan (PIRP) defines a framework for processes, communication, and roles and responsibilities for privacy incidents involving HUDs information and information systems. The PIRP ensures the proper procedures are in place to detect, analyze, respond, and recover from an actual, potential, or suspected privacy incident involving HUD's information and information systems.

The objective of the PIRP is to protect HUD's data, minimize loss or theft of information, and prevent disruption of critical services when incidents occur.

To accomplish this objective, it is necessary to:

- Coordinate proactive activities to reduce the risk of privacy compromise, including abiding by HUD Privacy policies and best practices;
- Be aware of each individual's role and responsibilities in the incident reporting process;
- Understand and adhere by incident response procedures and ensure necessary parties are notified in a timely manner.

While the Cyber Incident Response Plan (CIRP) provides an approach for handling cyber-specific threats, the PIRP applies to *all* privacy related threats, both cyber and non-cyber. Although most incidents involve information technology, a privacy incident may also involve verbal exchange, paper handling, and or physical security.

Scope

The HUD PIRP applies to all HUD personnel (including contractors) with access to HUD information and information systems in any format.

Authorities

Federal Statutes

- Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained on Individuals" [The Privacy Act of 1974, as amended]
- Title 6, U.S.C., Section 142, "Privacy Officer"
- Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014, as amended (FISMA)]

OMB Regulations and Guidelines

- Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources (updated July 28, 2016)
- OMB Memorandum 16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)
- OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

Definitions

Privacy Incident

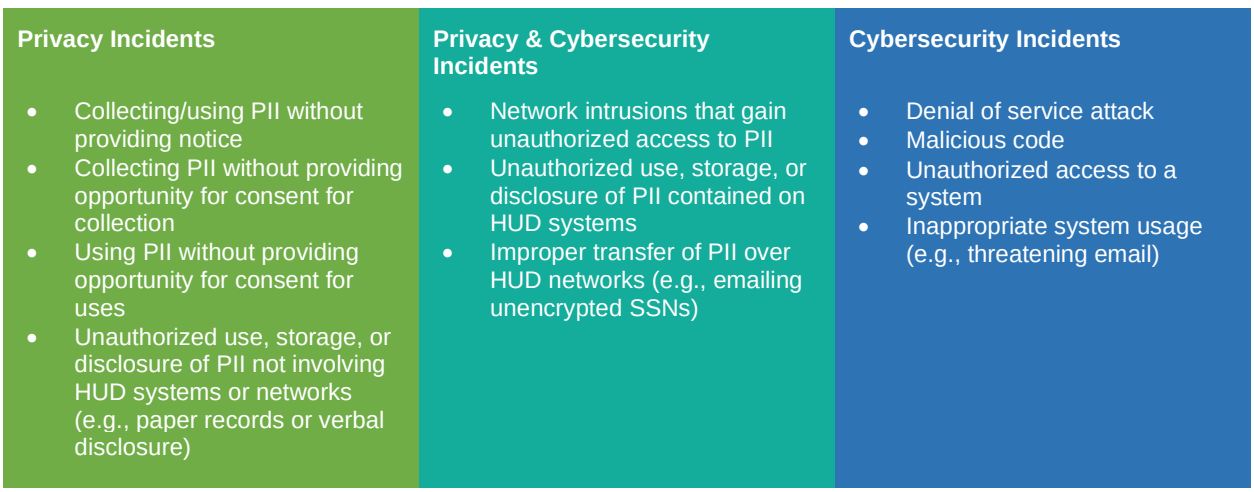
A privacy incident as defined by OMB Memorandum 17-12 is "An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security playbooks, or acceptable use policies."

There are many types of privacy incidents, including but not limited to using PII for purposes other than the stated purpose for which the information was originally collected, exceeding the retention period for PII, and collecting and/or using PII without first providing proper notice. The term privacy incident encompasses *both suspected and confirmed incidents* involving PII and applies to information in *both electronic and paper format*.

Cybersecurity Incident

A cybersecurity incident as defined by NIST Special Publication (SP) 800-53 Revision 4 is "any occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or, constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." Not all security incidents are privacy incidents and, conversely, not all privacy incidents are security incidents, but some incidents can be both a privacy incident and a security incident, as shown in the box in the center of Figure 1. Note that while this is intended to be a representative sample, this is not intended to be an exhaustive list.

Figure 1: Cybersecurity vs. Privacy Incidents



Personally Identifiable Information (PII)

For the purposes of this guidance, PII is defined as information which can be used to distinguish or trace a data subject's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Some examples include full names, social security numbers, telephone numbers, credit card numbers, driver's license numbers and biometric identifiers. Please refer to the HUD Privacy Policy for details regarding examples of PII and general guidance on proper PII handling.

Privacy Incident Response Procedures

Initial Discovery and Reporting

Once discovered, **HUD personnel** should report all privacy and cybersecurity incidents that are either suspected and/or confirmed to their **Office manager**.

- If you are unsure if something is an incident, report it to your **Office manager** and ask for assistance.
- If you are unable to reach your **Office manager**, call the **HUD Help Desk** at 1-888-297-8689 (Select Option 9 for assistance).

Office managers should coordinate with their **Privacy Liaison Officers (PLOs)**, **Security Operations Center (SOC)**, and the **HUD Help Desk** to determine if the incident is a privacy incident, cyber incident, or both.

- Contact the **HUD Help Desk** at 1-888-297-8689 (Select Option 9 for assistance).
- Contact **SOC** at cirt@hud.gov

Responding to Privacy Incidents

All incidents that are determined to be privacy incidents (cyber and non-cyber) should be reported to the Privacy Office. Office managers should complete and submit the HUD Privacy Incident Report as explained below *within one hour of discovering the incident.*

The HUD Privacy Incident Report should be sent to the Privacy Office at privacy@hud.gov.

HUD Privacy Incident Report

The PLOs for the Office where the incident occurred should fill out the HUD Privacy Incident Report Template. The report should include basic facts regarding when the incident occurred, when the incident was discovered, information about the nature of the incident, and whether the suspected incident involves PII. If the incident was also a cybersecurity incident, include the HUD system identifiers for all systems involved in the incident.

The PLOs for each Office are responsible for overseeing the documentation process and coordinating with Office managers and personnel to ensure all necessary information is collected and reported to the Privacy Office. While not all information may be available at the outset, the affected Office should gather as much information as possible for submission to the Privacy Office *within one hour of discovery.*

Responding to Cyber Privacy Incidents

In addition to the HUD Privacy Incident Report, if the privacy incident is also a cybersecurity incident, please refer to the HUD (CIRP) and coordinate with **SOC** for further steps.

- Contact **SOC** at cirt@hud.gov

Privacy Incident Roles and Responsibilities

HUD Breach Notification Response Team (HBNRT)

The HUD Breach Notification Response Team (HBNRT) is a core group of HUD privacy stakeholders responsible for managing a privacy incident lifecycle, including preparation, detection and risk analysis, triage and escalation, response and recovery, and coordination of any post-incident activities with the HUD CIRT.

In collaboration with the Privacy Office, the HBNRT is responsible for involving other key stakeholders to assist with the appropriate follow-up after a privacy incident and for escalating and/or notifying an incident alert and involving other entities within HUD and other key officials within stakeholder organizations as necessary. The HUD Breach Notification Policy and Response Plan (HBNRP) outlines HUD's full approach for coordinating a response to a privacy incident.

General Personnel

- All **HUD personnel** should report actual and suspected privacy and cybersecurity incidents to their **Office manager**.
- After initial reporting, **HUD personnel** should also coordinate with **Office managers**, **PLOs**, and **SOC** as necessary to respond to incidents and breaches.

Office Managers

- **Office managers** are responsible for coordinating with **PLOs**, the **HUD Help Desk**, and **SOC** to determine whether an incident is a privacy incident, cybersecurity incident, or both.
- After initial reporting, **Office managers** should also coordinate with **PLOs**, the **Privacy Office**, **SOC**, and the **HBNRT** as necessary to respond to incidents.

PLOs

- **PLOs** should coordinate with **Office managers**, the **HUD Help Desk**, **SOC**, and the **Privacy Office** to assess what kind of incident occurred and how to properly report and document the incident.
- **PLOs** are responsible for ensuring incidents that occur within their Offices are properly reported to the **Privacy Office** via the HUD Privacy Incident Report template.